What is claimed is:

1. An identification document comprising a photographic representation of a bearer of the identification document and indicia provided on the document, the identification document further comprising a security feature printed on a surface of the identification document in a two-dimensional symbology, the security feature including:

a first set of information corresponding to at least one of the identification document, the bearer of the identification document and an issuer of the identification document, wherein the first set of information comprises an unencrypted form; and

a cryptographic measure associated with the first set of information, the cryptographic measure identifying at least a record of fabrication for the identification document.

2. The identification document of claim 1, wherein the record of fabrication identifies at least one of equipment used in fabricating the identification document, an identification document assembler, a distribution channel and an operator of document fabrication equipment.

3. The identification document of claim 1, wherein the first set of information comprises at least one of a document identifier, issuer identification, issue date, bearer's date of birth, characteristics associated with the bearer's physical attributes, bearer's name, address, document inventory number and bearer's age.

4. The identification document of claim 1, wherein the two-dimensional symbology comprises at least one of a 2D-barcode, data glyph, maxicode, PDF 417, DataMatrix, and QR Code.

5. The identification document of claim 1, wherein the cryptographic measure comprises an encrypted form corresponding to a private key, said cryptographic measure further comprising at least one of a public key associated with the private key and information identifying where a public key associated with the private key can be obtained, wherein the private key is uniquely associated with an element of the record of fabrication.

6. The identification document of claim 1, wherein said cryptographic measure comprises a cryptographic certificate.

7. The identification document of claim 6, wherein the certificate comprises a public key for decrypting at least a portion of the cryptographic measure.

8. The identification document of claim 6, wherein the cryptographic measure comprises an encrypted form corresponding to at least a first private key and second private key, wherein the first private key is uniquely associated with a fabrication equipment operator, and the second private key is uniquely associated with equipment used in fabricating the identification document.

9. The identification document of claim 6, wherein the cryptographic measure comprises at least a first digital signature and a second digital signature, wherein the first digital signature corresponds to a first stage of a document fabrication process, and the second digital signature corresponds to a second stage of the document fabrication process.

10. The identification document of claim 6, wherein the cryptographic measure comprises a hash of at least the first set of information, the hash being encrypted by the private key.

11. The identification document of claim 10, wherein the hash further represents a second set of information, wherein the second set of information is supplemental to the first set of information.

12. The identification document of claim 11, wherein the second set of information comprises a condensed representation of the photographic representation.

13. The identification document of claim 11, wherein the second set of information comprises a document inventory number, the inventory number being conveyed by a machine-readable code carried by the identification document.

14. The identification document of claim 1, wherein the indicia comprises at least one of artwork, text, barcodes, graphics and digital watermarking.

15. A method of analyzing an identification document, the identification document comprising a first set of information and a cryptographic signature corresponding to the first set of information, wherein the first set of information and the cryptographic signature are encoded in a machine-readable format, the encoding being printed or engraved on a surface of the identification document, said method comprising:

machine-sensing the first set of information and the cryptographic signature; and

determining fabrication details of the identification document from at least the cryptographic signature.

16. The method of claim 15, wherein the machine-readable format comprises digital watermarking.

17. The method of claim 15, wherein the machine-readable format comprises a two-dimensional symbology.

18. The method of claim 15, further comprising determining whether the identification document is deemed suspect based at least on the cryptographic signature.

19. The method of claim 18, wherein the identification document further comprises a certificate corresponding to the cryptographic signature, and wherein the certificate is encoded in the machine-readable format and printed or engraved on the surface of the identification document.

20. The method of claim 19, wherein said determining comprises determining whether the certificate has been revoked.

21. The method of claim 19, wherein said cryptographic signature comprises a date indicator, and wherein said determining comprises determining whether the date indicator corresponds with an untrusted date, and wherein at least a portion of the certificate is used to determine the untrusted date.

22. The method of claim 18, wherein the cryptographic signature corresponds with a symmetrical key, and said determining step comprises communicating at least the first set of information and the cryptographic signature to a remote processor, the remote processor determining whether the identification document is suspect by at least decrypting the cryptographic signature with the symmetrical key.

23. The method of claim 18, wherein the cryptographic signature corresponds to a pair of asymmetrical keys.

24. The method of claim 18, wherein the fabrication details comprise at least one of an identification document distribution record, unauthorized issuance, type of identification document, equipment used to fabricate the document, document assembling equipment operator, document lot number and document batch number.

25. The method of claim 18, wherein the fabrication details comprise at least a type of identification document, with a unique private key corresponding to the type.

26. The method of claim 15, further comprising verifying the first set of information with the cryptographic signature.

27. A method of identifying unauthorized issuance of an identification document, wherein unauthorized issuance occurs when the identification document is fabricated on authorized equipment but is issued in an unauthorized manner, the identification document including first data and a digital signature corresponding to at least the first data, the digital signature further including a date indicator associated with the fabrication of the identification document, said method comprising:

machine-sensing the identification document to obtain the first data and the digital signature;

validating the digital signature in accordance with a certificate associated with the digital signature;

determining whether the certificate has been revoked, and if so revoked,

determining whether the date indicator corresponds with a date associated with the certificate's revocation, and if so associated,

identifying the identification document as being issued without authority.

28. The method of claim 27, wherein the identification document further includes the certificate.

29. A method to establish whether an identification document should be trusted comprising:

randomly or pseudo-randomly selecting a unique serial number;

associating the unique serial number and fabrication details in a data record;

providing the unique serial number on the identification document; and

issuing the identification document.

30. The method of claim 29, wherein the serial number is provided on the identification document in the form of a machine-readable code.

31. The method of claim 29, wherein the machine-readable code comprises at least one of a digital watermark and a 2D-symbology.

32. The method of claim 29, wherein the fabrication details comprise at least one of fabrication operator, fabrication station, equipment used in fabrication, materials used in fabrication, and fabrication completion.

33. A method of binding a first feature to a second feature, the first and second features to be provided on an identification document, said method comprising:

receiving the first feature, the first feature comprising unique characteristics;

receiving the second feature, the second feature including a first data set;

computing a cryptographic signature over the first data set and the unique characteristics;

appending the cryptographic signature and information associated with the cryptographic signature to the first data set;

printing the first feature on the identification document;

printing the second feature including the appended first data set on the identification document.

34. The method of claim 33, wherein the first feature comprises a photographic representation of a bearer of the identification document.

35. The method of claim 34, wherein the unique characteristics comprise at least one of a digital watermark embedded in the photographic representation and a hash of the photographic representation, and wherein the second feature comprises a machine-readable symbology.

36. The method of claim 35, wherein the information corresponds to at least one of a certificate, a public key and instructions on how to obtain a public key.

37. A method of identifying unauthorized issuance of an identification document, wherein unauthorized issuance occurs when the identification document is fabricated on authentic equipment, but is issued in an unauthorized manner, the identification document including first data and a digital signature corresponding to at least the first data, said method comprising:

obtaining the first data and the digital signature;

validating the digital signature in accordance with a public key associated with the digital signature; and

determining whether the public key is associated with unauthorized issuance; and if so associated,

identifying the identification document as being issued without authority.

38. The method of claim 37, wherein the digital signature further includes a date indicator associated with fabrication of the identification document, and said determining step comprises comparing the date indicator to a date associated with the unauthorized issuance.

39. The method of claim 37, comprising machine reading the first data and digital signature.

40. The method of claim 37, wherein the identification document further includes at least one of a certificate, the public key, and information to identify the public key.

41. The method of claim 37, wherein authentic equipment comprises equipment that is the same as equipment used to produce authentic documents.